Operational Resiliency Management

An Introduction to the Resiliency Engineering Framework

Rich Caralli – SEI

Charles Wallen - FSTC

Federal Reserve Bank Business Continuity Conference

20 September 2006

Report Documentation Page		Form Approved OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **20 SEP 2006**	2. REPORT TYPE	3. DATES COVERED **00-00-2006 to 00-00-2006**
4. TITLE AND SUBTITLE **Operational Resiliency Management: An Introduction to the Resiliency Engineering Framework**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University ,Software Engineering Institute (SEI),Pittsburgh,PA,15213**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release; distribution unlimited**		
13. SUPPLEMENTARY NOTES		
14. ABSTRACT		
15. SUBJECT TERMS		

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**42**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Agenda

Who are we?

Introduction to Operational Resiliency and the Resiliency Model

Characterizing the Problem Space .

Introducing the Resiliency Engineering Framework

Summary

Questions

Financial Services Technology Consortium

Established in 1993

Member-owned consortium for collaboration between financial services-focused organization

Explore new technologies and methodologies to address today's business requirements   .

Projects:

- Technology Review

- Compliance

- Business Continuity Maturity Model

Software Engineering Institute

Established in 1984

Federally Funded Research and Development Center (FFRDC)

College-level unit of Carnegie Mellon University

Includes five technical programs aimed helping defense, government, industry, and academic organizations to continually improve software-intensive systems

Widely-known "brands"

- CERT Coordination Center
- Capability Maturity Model Integration (CMMI)
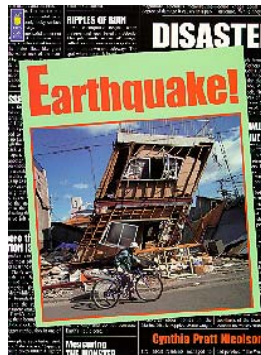
Managing Today's Operational Risk Challenges

Regulations

Cyber Security

Terrorism

Disasters

Resiliency Engineering

An Emerging Management Discipline

Supply Chain

Infrastructure

Resiliency…more than a buzzword

Resiliency is the ability of an object to return to its original shape

Operational resiliency refers to an organization's ability to function and adapt through the lifecycle of disruptions

A resiliency model is a roadmap for managing the consistent delivery of products and services

Software Engineering Institute | Carnegie Mellon

Managing resiliency

Requires

- Ongoing measurement and monitoring

- Balancing cost and risk tradeoffs

- Taking an enterprise focus

Financial Services organizations recognize a need to be able to manage resiliency in a systematic, consistent, measurable, and improvable way

Software Engineering Institute | Carnegie Mellon

A model is needed to. . .

Identify and prioritize risk exposures

Define a process improvement roadmap

Measure and facilitate strategic planning

Address interdependencies

Promote pro-active regulatory compliance

Goal: continuous improvement of resiliency processes
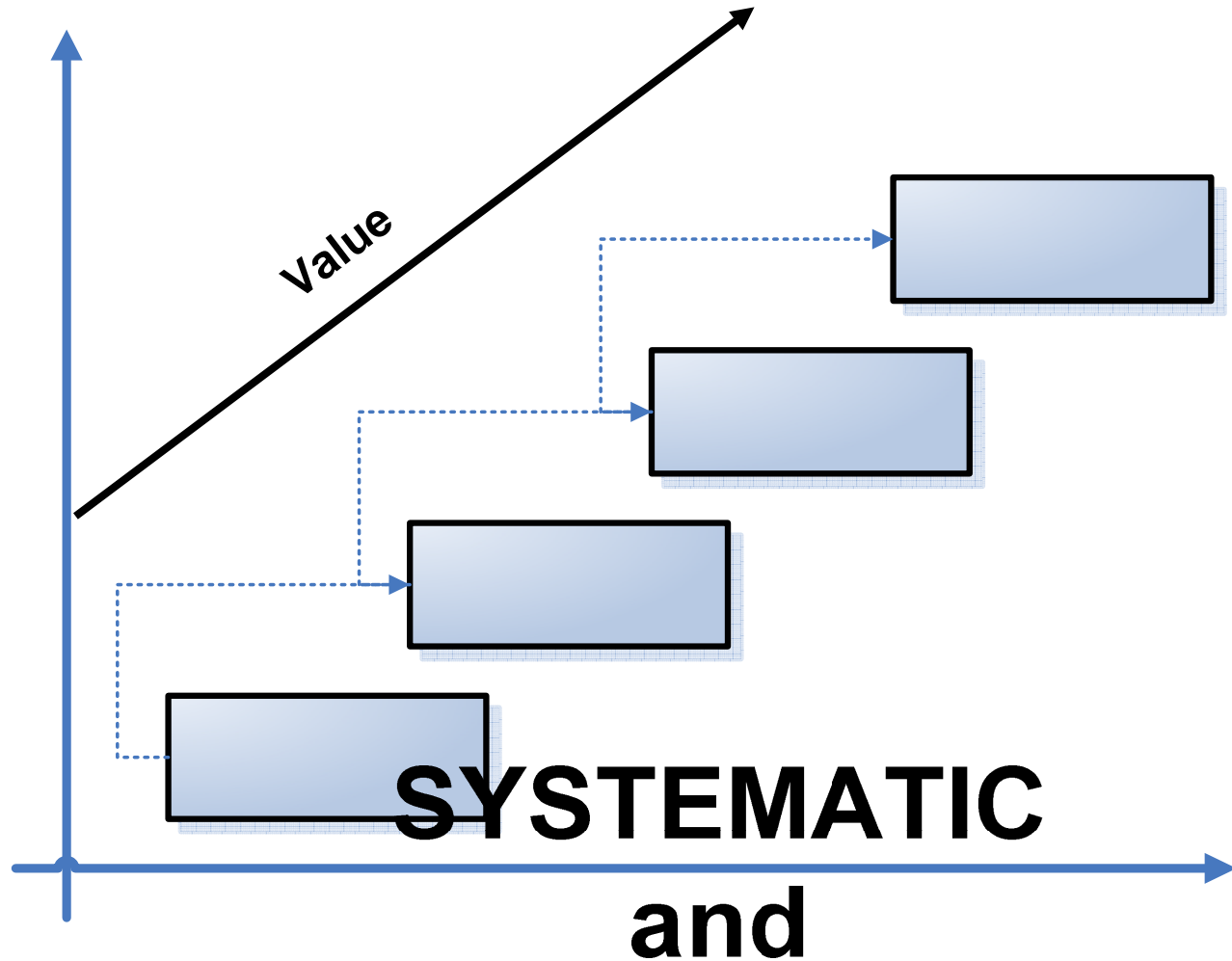
Why use a "model" approach?

Provides an operational risk roadmap

Vendor-neutral, standardized, unbiased assessment vehicle

Can be leveraged for process improvement at any organization, public or private

Avoids the pitfalls of prescriptive solutions by promoting resiliency engineering and the use of organization-appropriate practices

Teaming with the SEI

Fieldwork history with OCTAVE^{SM}

Best-in-Class IT Operations Roundtable

Enterprise Security Management and PrISM

Resiliency Maturity Model

Resiliency Engineering Framework

CERT | **Software Engineering Institute** | **Carnegie Mellon**

Defining the problem

Typical organizational approach to operational risk management activities:

- Poorly planned and executed function

- Business units not involved

- No asset management function

- Seen as a technical function or responsibility

- Searching for magic bullet: CobiT, ITIL, ISO17799, NFP1600

- Poorly defined and measured goals

- Funding model reactive, not strategic

Organizational impact

Misalignment of operational, security, and continuity goals

False sense of accomplishment

Failure to recognize/utilize all skills/resources

Compliance at the expense of effectiveness

Static, inflexible approach that can't evolve

The changing view of security

Security is an operational risk management activity

Security has two purposes:

- Prevent disruption to core business drivers

- Sustain the survivability of the organization's mission

Security is not an end, but a means to achieving higher organizational goals

Operational risk and resiliency

Operational risk is the risk that results from

- Failed internal processes

- Inadvertent or deliberate actions of people

- Problems with systems and technology

- External events

Operational resiliency is the organization's ability to sustain the mission in the face of these risks

Managing operational resiliency

Requires more than traditional security activities

Continuity of operations (COOP) planning is essential

Derives benefits from process excellence in areas such as IT operations and service delivery management

Security and operational resiliency

Focus on keeping critical assets safe from harm

Limiting threats and managing impacts

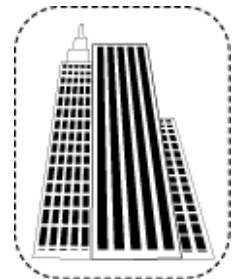Manage confidentiality, integrity, and availability

Manage "condition"

people
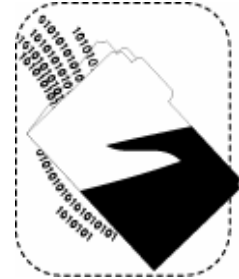
information

technology

facilities

Business continuity and operational resiliency

Limit unwanted effects of realized risk

Ensure availability and recoverability

Manage "consequence"

people

information

technology

facilities

Software Engineering Institute | Carnegie Mellon
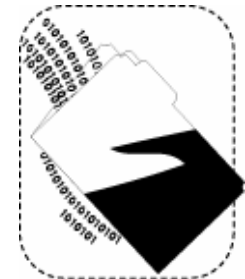
IT Operations Management and operational resiliency

Limit vulnerabilities and threats that originate in the technical infrastructure

Ensure availability and recoverability of technology

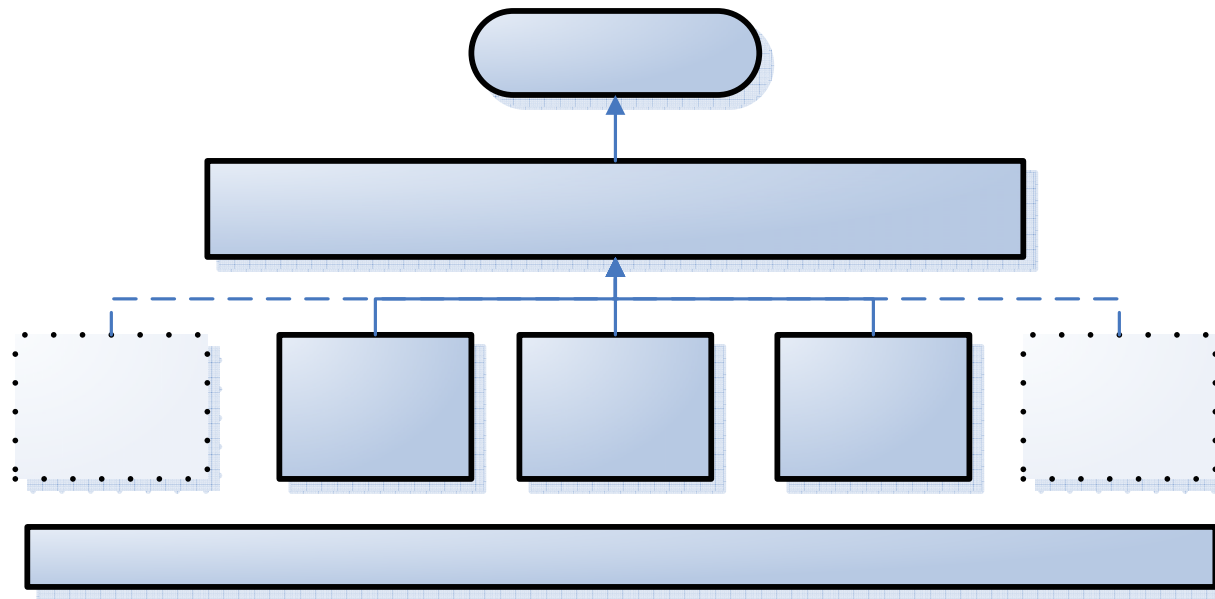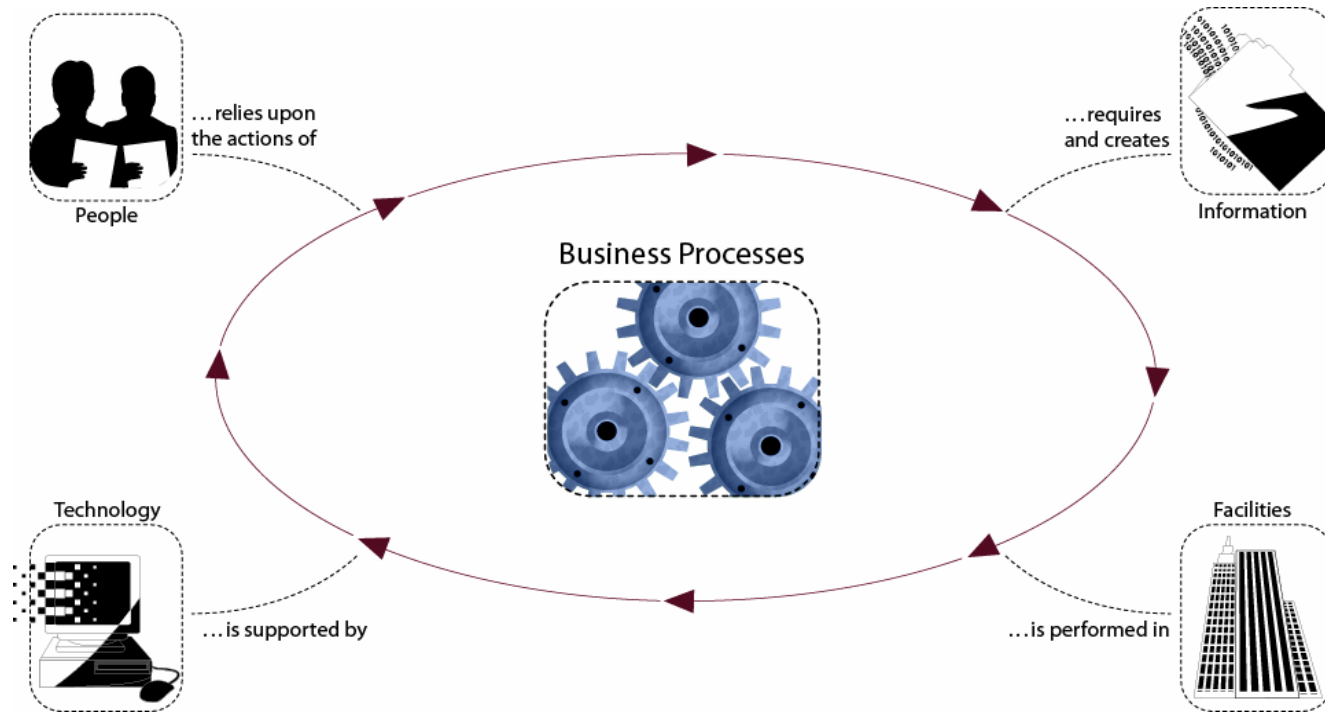technology

information

Collaborating toward a common goal

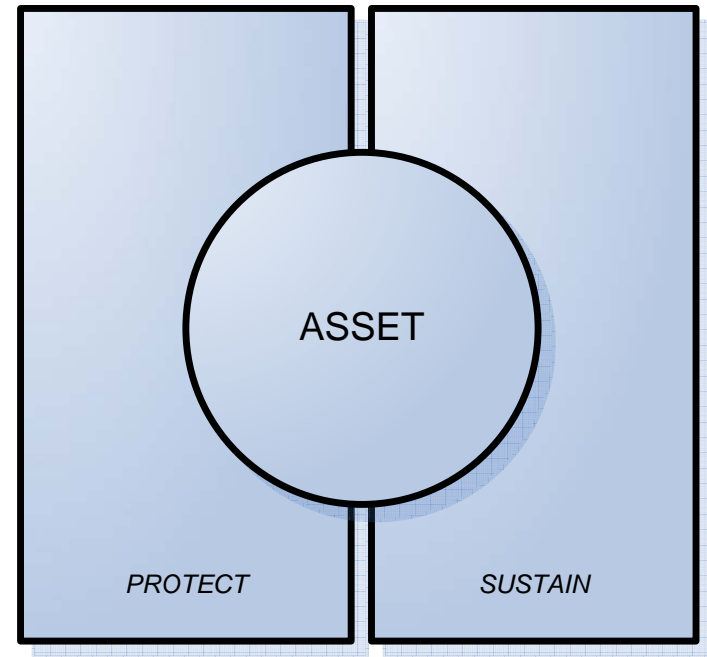# Operational resiliency in practice

An emerging holistic view

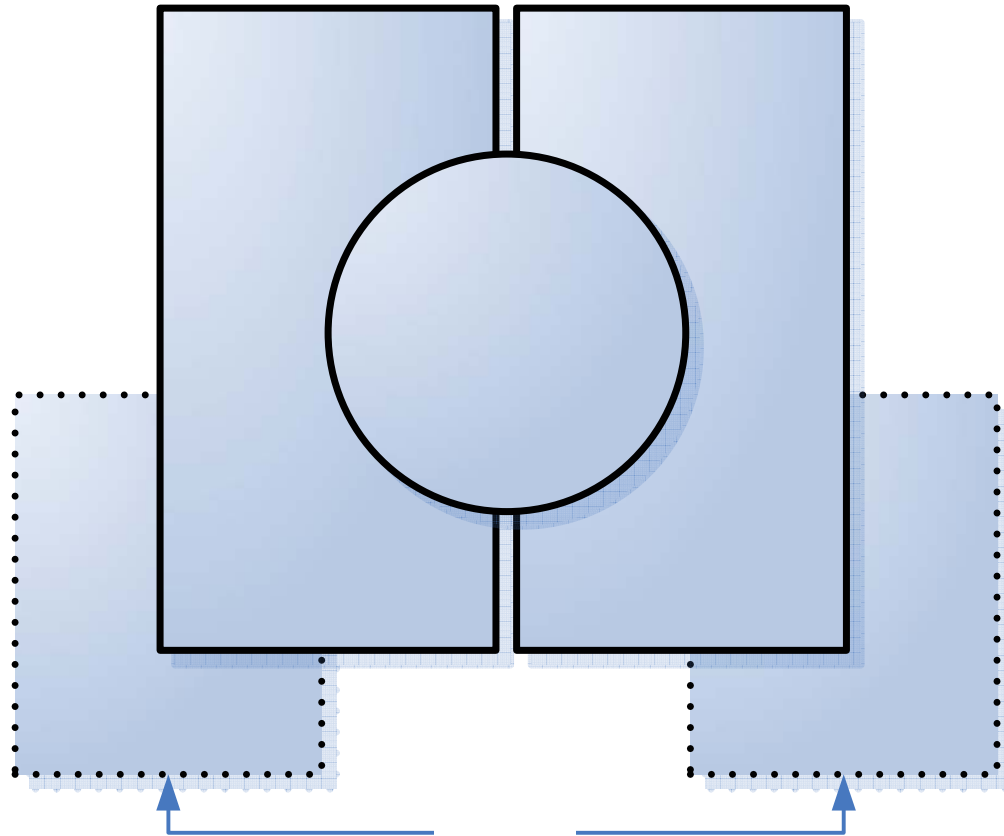Organization is dependent on the productivity of four assets:

- People

- Information

- Technology

- Facilities

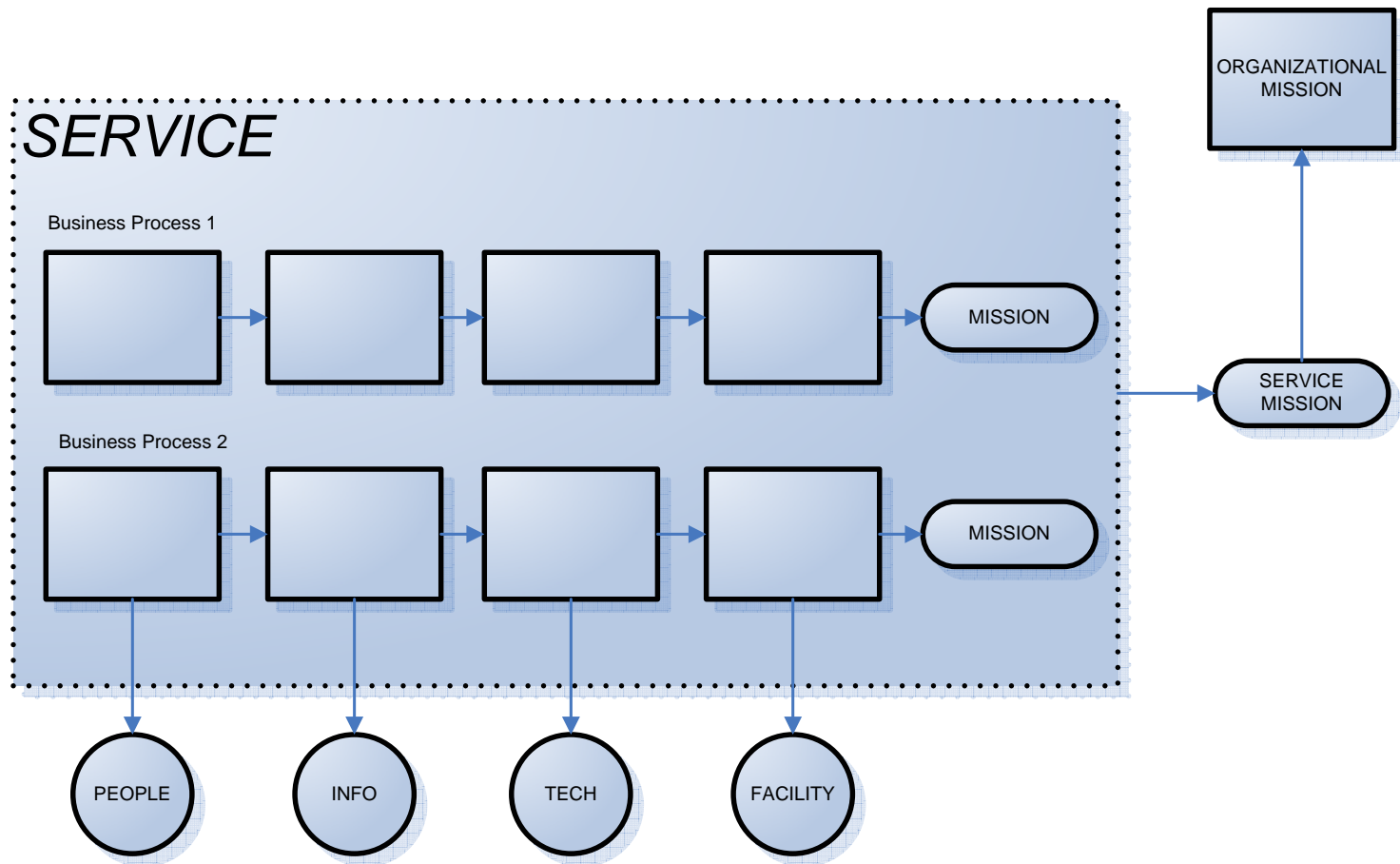Each asset must be protected and sustainable

PROTECT | SUSTAIN | ASSET

Collaborating toward a common goal

Focusing on the mission

How do we get there?

Organizations are not structured today to facilitate collaboration toward a common goal of resiliency

- Deficient funding models

- Management direction and oversight lacking

- Practice-driven

- Compliance-focused

Need to view resiliency as a definable, manageable, enterprise-wide process

Considering a process approach

Elevating the management and coordination of operational-resiliency focused activities to the enterprise level

- Shared goals and resources

- Elimination of redundancy and stovepipes

- Elimination of framework quagmire through practice integration

- Measuring process effectiveness

- Moving toward process improvement

How does process differ from practice?

Process

- *Describes* the "what"

- Set and achieve process goals

- Manage process to requirements

- Select practices based on process goals

- Can be defined, communicated, measured, and controlled

Practice

- *Prescribes* the "how"

- No practice goals

- Tends toward "set and forget" mentality

- Reinforces domain-driven approach

- One size does not fit all

- Regulatory vehicle

The relationship between process and practice
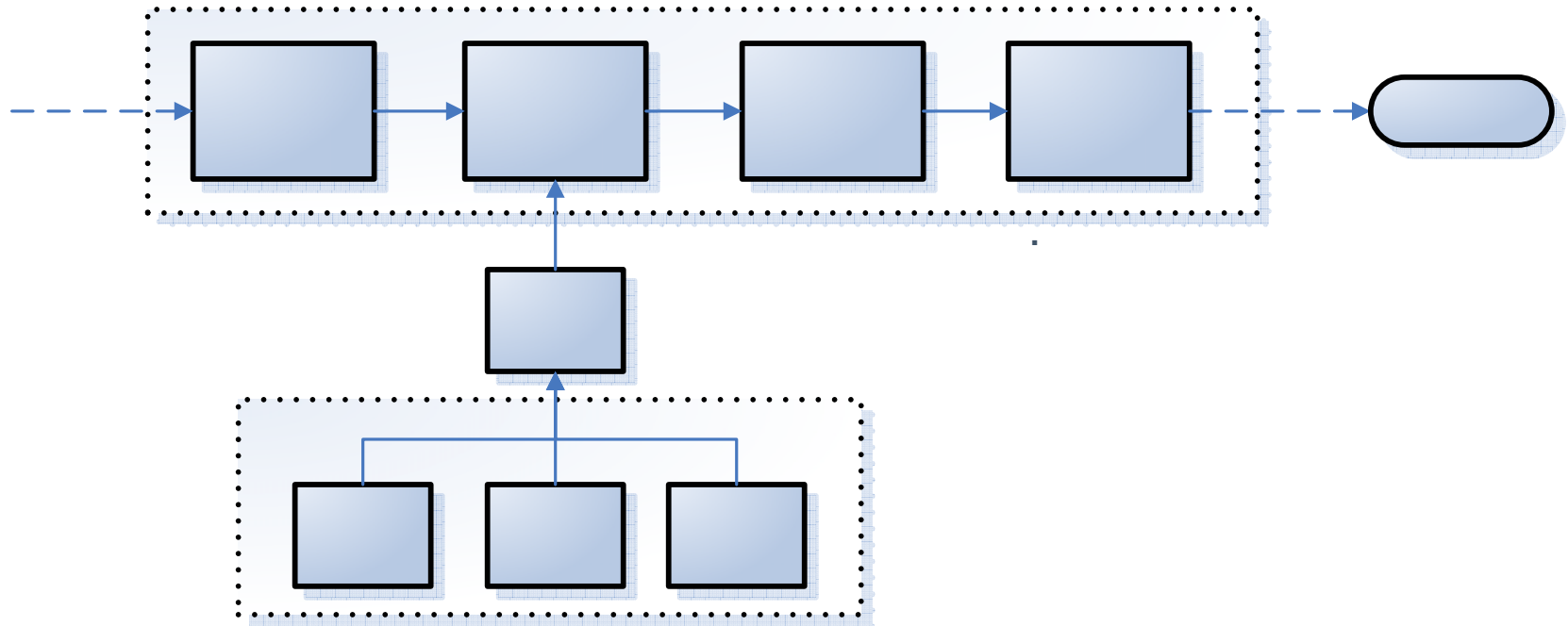
Embracing process improvement

Improvement in meeting resiliency goals is dependent on the active management of the process

Process maturity increases capability for meeting goals and sustaining the process

.

"Are we resilient?" or *"Are we secure?"* is answered in the context of goal achievement rather than what hasn't happened

Meaningful, purposeful selection and implementation of practices

Resiliency engineering defined

The process by which an organization establishes, develops, implements, and manages the operational resiliency of services, related business processes, and associated assets

"Requirements-driven security and COOP"

Introducing the Resiliency Engineering Framework

The Resiliency Engineering Framework

A process improvement framework for security and continuity of operations

Defines basic process areas and provides guidelines for improving security and COOP processes

Addresses operational risk management through process management

Vital linkages between security, COOP, and I/T ops are captured in the process definition

Establishes a capability benchmark

Framework architecture

Represents processes that span four basic areas:

- Enterprise management

- Engineering

- Operations management

- Process management

Considers the resiliency of people, information, technology, and facilities in the context of services and business objectives

Enterprise management processes

Enterprise capabilities that are essential to supporting the resiliency engineering process

RSKM – Risk Management

EF – Enterprise Focus

COMP – Compliance Management

FRM – Financial Resource Management

HRM – Human Resource Management

Operations management processes

Capabilities focused on sustaining an adequate level of operational resiliency

SAM – Supplier Agreement Management

SRM – Supplier Relationship Management

AMC – Access Management and Control

IMC – Incident Management and Control

VM – Vulnerability Management

EC – Environmental Control

KIM – Knowledge and Information Management

SOM – Security Operations Management

ITOPS – IT Operations Management

Engineering processes

Capabilities focused on establishing and implementing resiliency for organizational assets, business processes, and services

RD – Requirements Definition

RM – Requirements Management

AM – Asset Management

COOP – Continuity of Operations Planning

REST – Restoration of Operations Planning

CSI – Control Selection and Implementation

RAD – Resilient Architecture Development

Process management processes

Enterprise capabilities related to defining, planning, deploying, implementing, monitoring, controlling, appraising, measuring, and improving processes

OT – Organizational Training

OPF – Organizational Process Focus

OPD – Organizational Process Definition

MA – Measurement and Analysis

MON - Monitoring

Using the framework

Establish current level of capability

Set forward-looking resiliency goals and targets

Develop plans to close identified gaps

Build resiliency into important assets and architectures

Reduce reactionary activities; shift to directing and controlling activities

Align common practices with processes to achieve process goals

Where do we go from here?

Release REF v1.0 in October 2006 for comments

Guidelines for improving the security and business continuity processes

Phase III expansion of model development and piloting

Exploration of integration with other existing models

Development of appraisal methodology to measure capability for managing resiliency

Phase I and Phase II Project Members

Ameriprise

Bank of America

Carnegie Mellon

Capital Group

Citicorp

Discover

DRII

DRJ

IBM

JPMorgan Chase

Key Bank

KPMG

MasterCard

Marshall and Ilsley

NY Federal Reserve Bank

SunGard

Trizec Properties

US Bank

Wachovia

Summary and questions

Operational resiliency must be actively managed

Security, BC/DR, and ITOps must collaborate

Model-based process improvement brings defined, systematic, repeatable, consistent, and improvable processes

Approach must be flexible and adaptable

No one-size-fits-all solution

For more information

Rich Caralli

Software Engineering Institute

www.sei.cmu.edu

www.cert.org

rcaralli@cert.org

Charles Wallen

Financial Services Technology Consortium

www.fstc.org

charles.wallen@fstc.org